EFFICIENT MANAGEMENT AND BLOCKING OF MALICIOUS CODE AND HACKING ATTEMPTS IN A NETWORK ENVIRONMENT

ABSTRACT

A system, method and computer program product are provided for preventing an outbreak of malicious code. First, malicious code is identified at a local location on a network. Information relating to the malicious code, such as type, context, protocol, severity, reporting server, and IP address, is encrypted at the local location. The encrypted information relating to the malicious code is sent to a plurality of remote locations utilizing the network. Instances of the malicious code are blocked at the remote locations for a predetermined amount of time based on the information. Another system, method and computer program product are provided for preventing an outbreak of malicious code. Accordingly, malicious code is identified at a local location on a network. Information relating to the malicious code is gathered at the local location and sent to a remote location utilizing the network. Such information includes a type, context, protocol, severity, reporting server, and/or source of the malicious code. Instances of the malicious code are blocked at the remote location is restricted. A system, method and computer program product for denying access to a hacker is also provided according to one embodiment. An attack by a hacker is identified at a local location on a network. Information relating to the attack is encrypted at the local location. Such information can include a type, context, protocol, severity, reporting server, and/or IP address associated with the attack. The encrypted information relating to the attack is sent to a plurality of remote locations utilizing the network. Access to the remote locations is restricted for a predetermined amount of time based on the

information. In another system, method and computer program product, a method for denying access to a hacker is provided according to one embodiment. An attack by a hacker at a local location on a network is identified. Information relating to the attack at the local location is gathered and sent to a remote location utilizing the network. Access to the remote location is restricted. Again, the information can be a type, context, protocol, severity, reporting server, and/or source of the attack.